

PRIVACY POLICY

WS Telecom Inc.

Effective Date: June 22, 2026

Version: 1.0

Jurisdiction: State of Wyoming, USA

1. INTRODUCTION

WS Telecom Inc. ("Company", "We", "Us") respects your privacy. This Privacy Policy explains how we collect, use, and protect data when you use our services or visit our website.

2. DATA CONTROLLER & RESPONSIBILITY

- **Controller:** WS Telecom Inc., 1309 Coffeen Avenue STE 1200, Sheridan, WY 82801
 - **EU Representative:** (if applicable, to be designated)
 - **DPA:** Data Processing Agreement available upon request (GDPR Article 28)
-

3. DATA WE COLLECT

3.1 Account Registration

- Name, email, phone number
- Company name, country, tax ID
- Billing address, payment method
- Account username and password (hashed)

3.2 Service Usage Data

- IP addresses accessed to services
- Bandwidth consumption and traffic patterns
- DNS queries and domain lookups
- Login timestamps and account activity

3.3 Network Traffic (Limited)

- Source/destination IP pairs
- Port numbers and protocol types

- Aggregate byte counts (not packet payload)
- Geo-location of traffic endpoints (derived from IP)

Limitation: Company does not inspect payload content except:

- Abuse/AUP violation investigation
- Law enforcement with valid warrant
- Security incident response

3.4 Support & Communication

- Support tickets and email correspondence
- Chat logs (support sessions)
- System generated logs (timestamps, actions)
- Call recordings (with consent, if applicable)

3.5 Website & Portal

- IP address and user-agent (via cookies)
- Pages visited, referrer, duration
- Search queries within portal
- Device type and browser type

3.6 Billing Data

- Payment method (last 4 digits only)
- Invoice history and payment receipts
- Refund requests and disputes

4. LEGAL BASIS FOR PROCESSING (GDPR)

Where GDPR applies:

Data Type	Legal Basis
Account registration	Contract performance
Service usage (for billing)	Contractual necessity
Network monitoring	Legitimate interest (security, AUP enforcement)

Support communications	Contract performance
Marketing (optional)	Explicit consent
Compliance/legal	Legal obligation

5. DATA RETENTION

Data Type	Retention Period
Account data	Duration of service + 7 years (tax law)
Billing/invoices	7 years (US tax requirement)
Support tickets	3 years
Network logs	90 days (aggregate)
Website cookies	Per cookie policy (60 days standard)
Deleted account data	30 days (verification period)

6. DATA SHARING

6.1 We Do NOT Share Personal Data

-
- We do not sell personal data
 - We do not share with third-party marketers
 - We do not use data brokers

6.2 We May Share With

Service Providers:

- Payment processors (to process charges)
- Email providers (to send notifications)
- Cloud storage (for backups)
- Accounting/audit firms (for compliance)

Legal Requirement:

- Law enforcement (subpoena, warrant, or valid legal process)

- Courts (judicial order)
- Regulators (FCC, SEC, state officials)
- OFAC (sanctions screening)

Security/Abuse:

- Network operators (DDoS mitigation, IP reputation)
- Abuse reporting services (phishing, malware ISPs)
- Law enforcement (criminal investigation, with process)

Data Processors:

- All processors sign Data Processing Agreements (GDPR Article 28)
- Processors may be located in EU, USA, or other jurisdictions
- International transfers comply with GDPR Chapter 5

7. INTERNATIONAL TRANSFERS

For EU residents: Personal data may be transferred to USA based on:

- Data Processing Agreement with Standard Contractual Clauses
- Risk assessment per GDPR and CJEU Schrems II
- No adequacy decision for USA; reliance on SCCs + safeguards

For California residents: CCPA notice under Section 1798.100 applies (see Section 10).

8. COOKIES & TRACKING

8.1 Cookie Types

Cookie	Purpose	Retention
session_id	Authentication	Session only
user_pref	Language, theme	1 year
analytics	Google Analytics (optional)	26 months
ads	Remarketing (disabled by default)	1 year

8.2 Cookie Consent

-
- Consent required before non-essential cookies (GDPR)
 - California consumers have "opt-out" right (CCPA)
 - Cookie banner displayed; consent recorded

8.3 Third-Party Analytics

- **Google Analytics:** ga.js; privacy policy: google.com/analytics/terms
 - **Disabled by default for EU**
 - Opt-out: tools.google.com/dlpage/gaoptout
-

9. YOUR RIGHTS

9.1 GDPR Rights (EU Residents)

- **Access:** Copy of personal data held (Art. 15)
- **Rectification:** Correct inaccurate data (Art. 16)
- **Erasure:** "Right to be forgotten" under conditions (Art. 17)
- **Restriction:** Limit processing (Art. 18)
- **Portability:** Export data in standard format (Art. 20)
- **Objection:** Opt-out from processing (Art. 21)
- **Complaint:** File with data protection authority (Art. 77)

Exercise: Request via privacy@ws.network; response within 30 days.

9.2 CCPA Rights (California Residents)

- **Know:** What data is collected (§1798.100)
- **Delete:** Request deletion (§1798.105)
- **Opt-Out:** Disable sale of personal data (§1798.120)
- **Non-Discrimination:** No retaliation for rights exercise (§1798.125)

Note: Company does not "sell" data as defined by CCPA.

Exercise: Request via privacy@ws.network; response within 45 days.

9.3 Data Subject Rights Process

1. Submit request with identification
 2. Company verifies identity (reasonable security)
 3. Response provided within timeframe
 4. Free of charge; annual access requests covered
 5. Complex requests may extend 60-day limit
-

10. CALIFORNIA RESIDENT DISCLOSURES (CCPA)

10.1 Right to Know & Delete

Per CCPA §1798.100 & §1798.105:

- You may request what personal information is collected
- You may request deletion of personal information
- We will confirm receipt within 10 days; respond within 45 days

10.2 Opt-Out of Sale

Per CCPA §1798.120:

- We do NOT sell personal information
- "Sale" excludes service provider transfers
- If we begin selling, opt-out mechanism will be provided

10.3 Right to Non-Discrimination

Per CCPA §1798.125:

- We will not discriminate based on rights exercise
 - Price/service terms remain unchanged
-

11. SECURITY MEASURES

11.1 Technical Safeguards

- TLS/SSL encryption for data in transit
- AES-256 encryption for data at rest
- Firewalls, intrusion detection, endpoint protection
- Regular penetration testing (annual)
- Vulnerability scanning (monthly)

11.2 Administrative Controls

- Access controls (least privilege)
- Employee background checks
- Confidentiality agreements (all staff)
- Incident response plan
- Security awareness training

11.3 Physical Security

- Locked data centers with biometric access
- Video surveillance

- Climate control and disaster prevention
- Off-site backups

12. BREACH NOTIFICATION

In case of data breach:

- Notify affected individuals within 72 hours (GDPR)
- Notify state attorney general (California)
- Provide: Date of breach, data types, remediation steps
- Exception: Encrypted or unreadable data (minimal risk)

13. CHILDREN'S PRIVACY

Our services are not directed to children under 13. We do not knowingly collect data from children. If discovered, we will delete within 30 days. Contact privacy@ws.network to report.

14. THIRD-PARTY LINKS

Our website may link to third parties. We are not responsible for their privacy practices. Review their privacy policies before providing data.

15. DATA RETENTION FOR LEGAL HOLDS

If Company receives legal hold notice (litigation, investigation), we retain relevant data beyond normal retention periods until legal process concludes.

16. CHANGES TO THIS POLICY

We may update this policy with 30 days' notice. Significant changes require explicit consent. Continued service use = acceptance of changes.

17. CONTACT

Privacy Officer: privacy@ws.network

Legal: legal@ws.network

Mailing Address:

WS Telecom Inc.

1309 Coffeen Avenue STE 1200

Sheridan, WY 82801

USA

Data Protection Authority (EU):

File complaint with your national DPA
(e.g., GDPR Article 77 supervisory authority)

Effective Date: June 22, 2026

Last Updated: June 22, 2026

Next Review: June 22, 2027